AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims, in which claims 1-3, 7-11, 14-17, and 19-21 are currently amended, and claims 22-24 are newly added.

1. (Currently Amended) A network system ~~that resists denial of service attacks on~~ providing ~~an access link to a destination host belonging to~~ a virtual private network (VPN), said network system comprising:

one or more egress ~~boundary~~ routers having connections to an access network including ~~the~~ an access link, wherein said one or more egress ~~boundary~~ routers transmit intra-VPN traffic ~~toward the~~ to a destination host belonging to the VPN from sources within the VPN within a first access network logical connection for intra-VPN traffic and all extra-VPN traffic ~~toward~~ to the destination host from sources outside the VPN within a second access network logical connection for extra-VPN traffic, separate from the first access network logical connection; and

a plurality of ingress ~~boundary~~ routers coupled to the one or more egress ~~boundary~~ routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented.

2. (Currently Amended) The network system of Claim 1, ~~and further comprising a Differentiated Services network coupling~~ wherein the at least one of the plurality of ingress ~~boundary~~ routers ~~and~~ or the at least one of the one or more egress ~~boundary~~ routers logically

partitions intra-VPN traffic and extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

3. (Currently Amended) The network system of Claim 1, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress ~~boundary~~ routers.

4. (Original) The network system of Claim 1, and further comprising the access network.

5. (Original) The network system of Claim 4, and further comprising a customer premises equipment (CPE) edge router to the access link.

6. (Original) The network system of Claim 5, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

7. (Currently Amended) The network system of Claim 1, wherein at least one of said plurality of ingress ~~boundary~~ routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic.

8. (Currently Amended) The network system of Claim 1, wherein said one or more egress ~~boundary~~ routers provide a plurality of different qualities of services to said intra-VPN traffic.

9. (Currently Amended) A network system, comprising:

an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

one or more egress ~~boundary~~ routers having connections to the access network, wherein said one or more egress ~~boundary~~ routers transmit intra-VPN traffic ~~toward~~ to the destination host via the first logical connection and all extra-VPN traffic ~~toward~~ to the destination host via the second logical connection; and

a plurality of ingress ~~boundary~~ routers coupled to the one or more egress ~~boundary~~ routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented.

10. (Currently Amended) The network system of Claim 9, ~~and further comprising a Differentiated Services network coupling~~ wherein the at least one of the plurality of ingress ~~boundary~~ routers ~~and~~ or the at least one of the one or more egress ~~boundary~~ routers logically partitions the intra-VPN traffic and the extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

11. (Currently Amended) The network system of Claim 9, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress ~~boundary~~ routers.

12. (Original) The network system of Claim 9, and further comprising a customer premises equipment (CPE) edge router to the access link.

13. (Original) The network system of Claim 12, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

14. (Currently Amended) The network system of Claim 9, wherein at least one of said plurality of ingress ~~boundary~~ routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic.

15. (Currently Amended) The network system of Claim 9, wherein said one or more egress ~~boundary~~ routers provide a plurality of different qualities of services to said intra-VPN traffic.

16. (Currently Amended) A method ~~of protecting~~ providing ~~an access link to a destination host belonging to~~ a virtual private network (VPN) ~~against denial of service attacks~~, said method comprising:

in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

communicating, from a plurality of ingress ~~boundary~~ routers to one or more egress ~~boundary~~ routers, intra-VPN and extra-VPN traffic destined for ~~said~~ a destination host belonging to the VPN, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted

utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic;

transmitting intra-VPN traffic from said one or more egress ~~boundary~~ routers ~~toward~~ to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress ~~boundary~~ routers ~~toward~~ to the destination host via the second logical connection, such that denial of service attacks on said access link originating from sources outside the VPN are prevented.

17. (Currently Amended) The method of Claim 16, wherein ~~said communicating comprises communicating utilizing~~ a Differentiated Services protocol is used to logically partition the intra-VPN traffic and the extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

18. (Original) The method of Claim 16, wherein a customer premises equipment (CPE) edge router is coupled between said access network and said destination host, said method further comprising:

at a physical port of the CPE edge router coupled to the access link, providing first and second logical ports; and

receiving intra-VPN traffic at the first logical port, and receiving extra-VPN traffic at the second logical port.

19. (Currently Amended) The method of Claim 16, and further comprising logically partitioning intra-VPN and extra-VPN traffic by at least one of said plurality of ingress ~~boundary~~ routers utilizing a plurality of tunnels.

20. (Currently Amended) The method of Claim 16, and further comprising said one or more egress ~~boundary~~ routers providing a plurality of different qualities of services to said intra-VPN traffic.

21. (Currently Amended) A method for ~~resisting denial of service attacks on an access link to a destination host included in~~ providing a ~~VPN~~ virtual private network (VPN), the method comprising ~~the steps of~~:

assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN;

assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN;

granting, to traffic having the first priority level at the access link, precedence of access to ~~the~~ a destination host belonging to the VPN over traffic having the second priority level; and

transmitting the intra-VPN traffic from one or more egress ~~boundary~~ routers ~~toward~~ to the destination host via a first logical connection, and transmitting all extra-VPN traffic from said one or more egress ~~boundary~~ routers ~~toward~~ to the destination host via a second logical connection.

22. (New) A method of communicating, comprising:

receiving a packet that is destined to a host within a virtual private network;

determining whether the packet is originated within the virtual private network or external to the virtual private network; and

forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network.

23. (New) The method of Claim 22, wherein the packet is an Internet Protocol (IP) packet, and the steps of receiving, determining and forwarding are performed at a customer premises router configured to process the IP packet.

24. (New) The method of Claim 22, wherein the packet over the first logical path is marked as a higher priority than the second logical path using a differentiated services protocol.